

Pasos para conectar y securizar una red empresarial

Contexto SD-WAN

La tecnología SD-WAN permite ofrecer una WAN mucho más flexible, dinámica y fácil de gestionar. Esto deriva en la creación de nuevas arquitecturas de red que introducen mejoras sustanciales a la experiencia de usuario y a la eficiencia en el uso de ancho de banda.

Sin embargo, hay empresas que, al migrar a una solución SD-WAN, necesitan asegurar que, a la par de la evolución de la WAN, haya una mejora en los mecanismos de seguridad de la red con el fin de que esta se mantenga protegida.



Pasos para converger una solución de ciberseguridad y una red SD-WAN

1

PROTEGER EL TRÁFICO ENTRE SUCURSALES:

Una red SD-WAN puede utilizar diversos y múltiples medios de transporte, en muchas ocasiones, enlaces de acceso a redes públicas como Internet. La seguridad más básica que se debe tener en una solución de SD-WAN es aquella que permita **asegurar la confidencialidad e integridad del tráfico entre sedes**. Se requiere una solución que permita cifrar la información que sale de cada sede de forma que no sea vulnerable ante intercepciones.

2

PROTEGER EL ACCESO DIRECTO A INTERNET:

Las soluciones de SD-WAN permiten utilizar eficientemente el ancho de banda de cada sede al gestionar el acceso directo a Internet desde cada una de ellas. Esto, sin embargo, supone nuevos puntos de vulnerabilidad ante ciber-ataques y requiere que cada sede cuente con **mecanismos de seguridad que, en redes tradicionales, solo tenían las sedes principales**.

3

HABILITAR LA COMUNICACIÓN SEGURA CON LA NUBE PÚBLICA:

Es importante proteger el acceso a las aplicaciones y servicios alojados en la nube pública. Una solución puede ser proteger estas redes virtuales a través de la misma tecnología de encriptación que el tráfico de las redes físicas. De esta forma, la **comunicación con la nube pública estará protegida** a través de la red SD-WAN.

4

CONSIDERAR LA SEGMENTACIÓN INTERNA:

Dentro de cada sede, también es importante mantener el tráfico segmentado, de forma que haya un **mecanismo de seguridad entre diferentes redes**. Como ejemplo, agregar seguridad entre la red de los usuarios y la red en la que esté alojado algún servicio. Esto puede incluso ayudar a que, cuando ingrese a la red un dispositivo de usuario comprometido, este no sea capaz de propagar el ataque hacia los servicios en la red.

5

ASEGURAR UNA VISIBILIDAD Y GESTIÓN CENTRALIZADA:

Controlar la solución SD-WAN de cada sede por separado sin el apoyo de una plataforma de gestión y visibilidad unificada, hace que la gestión sea inmanejable. Una plataforma unificada permite asegurar la consistencia entre las configuraciones de distintas sedes y **facilita la detección de vulnerabilidades e incidencias**.

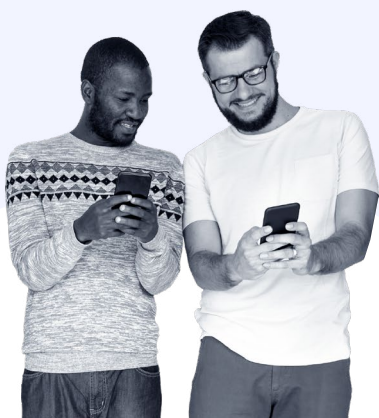
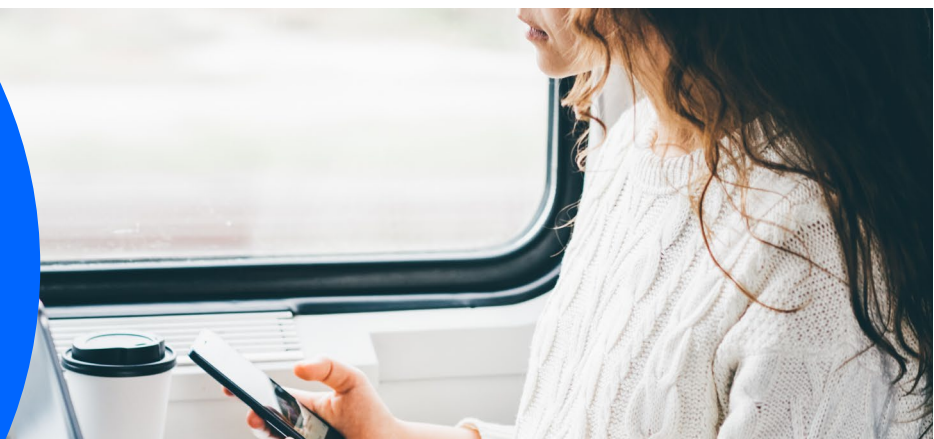
6

ASEGURAR LA CONVERGENCIA ENTRE SD-WAN Y CIBERSEGURIDAD:

Es importante asegurar que el servicio de SD-WAN y las funcionalidades de ciberseguridad son convergentes y no una integración de un servicio de seguridad en uno de SD-WAN. **El análisis por expertos de la coherencia de configuraciones y políticas de ambas tecnologías** será la clave para asegurar que no existen vulnerabilidades en la red empresarial. Además, poder correlacionar incidencias de SD-WAN y seguridad agilizará la identificación y resolución de éstas.

Para facilitar este camino, **el mercado ya ofrece soluciones para conectar y securizar la red empresarial a través de un único servicio**.

Estos servicios ofrecen tecnologías de SD-WAN convergente con funciones de ciberseguridad diseñadas y gestionadas por equipos de expertos que aseguran la coherencia entre las políticas de ambas soluciones.



Si tienes alguna duda o necesitas más información, contacta con tu comercial de Movistar más próximo.

Si lo prefieres, puedes contactarnos a través del siguiente enlace:

→ CONTÁCTANOS

2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. Todos los derechos reservados.

La información contenida en el presente documento es propiedad de Telefónica Cybersecurity & Cloud Tech S.L.U. (en adelante "Telefónica Tech") y/o de cualquier otra entidad dentro del Grupo Telefónica o sus licenciantes. Telefónica Tech y/o cualquier compañía del Grupo Telefónica o los licenciantes de Telefónica Tech se reservan todos los derechos de propiedad industrial e intelectual (incluida cualquier patente o copyright) que se deriven o recaigan sobre este documento, incluidos los derechos de diseño, producción, reproducción, uso y venta del mismo, salvo en el supuesto de que dichos derechos sean expresamente conferidos a terceros por escrito. La información contenida en el presente documento podrá ser objeto de modificación en cualquier momento sin necesidad de previo aviso. La información contenida en el presente documento no podrá ser ni parcial ni totalmente copiada, distribuida, adaptada o reproducida en ningún soporte sin que medie el previo consentimiento por escrito por parte de Telefónica Tech. El presente documento tiene como único objetivo servir de soporte a su lector en el uso del producto o servicio descrito en el mismo. El lector se compromete y queda obligado a usar la información contenida en el mismo para su propio uso y no para ningún otro. Telefónica Tech no será responsable de ninguna pérdida o daño que se derive del uso de la información contenida en el presente documento o de cualquier error u omisión del documento o por el uso incorrecto del servicio o producto. El uso del producto o servicio descrito en el presente documento se regulará de acuerdo con lo establecido en los términos y condiciones aceptados por el usuario de este para su uso. Telefónica Tech y sus marcas (así como cualquier marca perteneciente al Grupo Telefónica) son marcas registradas. Telefónica Tech y sus filiales se reservan todos los derechos sobre las mismas.

[Puedes consultar aquí nuestra política de privacidad](#)